Notice of Allowability	Application No.	Applicant(s)	
	09/739,219	SHIMOYAMA, TAKESHI	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 10/25/07*.

2. ☒ The allowed claim(s) is/are *1-3,5-10,12-15,18 and 19*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20071107* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. Claims 1-3, 5-10, 12-15, 18 and 19 are allowed. Claims 1-3, 5-10, 12-15, 18 and 19 are re-numbered as claims 1-15.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Temnit Afework on 11/7/07.

The application has been amended as follows:

Claim 1. (Currently Amended) A cipher designing apparatus for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits using a plurality of S-boxes, said cipher designing apparatus comprising:

an input unit inputting a memory capacity of a high-speed referable memory provided to said cipher device, an entire inputting and outputting bit number being input to and output from said cipher device, and a minimum input and output bit number of said S-boxes as an initial value;

a tentative decision unit dividing the entire input and output bit number by the initial value to acquire an integer quotient and an integer remainder, making a first set composed of the integer quotient pieces of the initial value, subtracting a number of one from the remainder

integer number, when the remainder integer number is not zero, and adding the subtracted number of one to the initial value in the first set one by one until the integer value remainder becomes zero, so as to acquire a second set composed of integer numbers, and tentatively deciding the integer numbers in the second set as a tentative inputting and outputting bit number of S-box;

a combining unit combining the integer numbers so as to make a third set of integer composed of combining integers;

a selecting unit determining how many pieces of the combined integers are in the third set, repeating the tentative deciding, combining and determining until a number of the combined integer numbers become equal to a final number that is calculated based on the memory capacity and the entire inputting and outputting bit number, and selecting, when the number of the combined integer numbers becomes equal to the final number, the combined integers of the third set to be an optimal combination of input and output bit numbers of each of the S-box;

a S-box generating unit generating a plurality of S-boxes each having the input and output bit number selected by said selecting unit.

Allowable Subject Matter

3. The following is an examiner's statement of reasons for allowance: The prior art of record discloses S-boxes where 8 input bits are transformed into 32 or 64 output bits and value of S-boxes is selected at random or to achieve certain properties of an encryption standard. However, the prior art of record does not explicitly disclose tentatively deciding, combining and determining until a number of the combined integer numbers becomes equal to a final number

that is calculated based on the memory capacity and the entire inputting and outputting bit number, and selecting, when the number of the combined integer numbers becomes equal to the final number, the combined integers of the third set to be an optimal combination of input and output bit numbers of each of the S-box in light of other features disclosed in independent claims 1, 8 and 15.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100